

CODES IN A_n LATTICES: GEOMETRY OF B_h SETS AND DIFFERENCE SETS

MLADEN KOVAČEVIĆ

ABSTRACT. Motivated by several communication scenarios, such as the permutation channel, the 0-insertion/deletion channel, and q -ary asymmetric channels, we investigate properties of (linear) codes in A_n lattices. In particular, we demonstrate a connection between such codes and notions of difference sets and B_h sets in Abelian groups. It is shown that the A_n lattice admits a linear perfect code of radius 1 if and only if there exists an Abelian planar difference set of cardinality $n+1$. Similarly, a direct link is given between linear codes of radius r in the A_n lattice and B_{2r} sets of cardinality $n+1$. B_{2r+1} sets are also represented geometrically in a slightly different way. Apart from providing a geometric intuition about B_h sets, this interpretation enables simple derivations of bounds on their parameters, which are either equivalent to, or improve upon the known bounds. In connection to the above, more general (non-planar) Abelian difference sets and perfect codes of radius r are also discussed.

1. INTRODUCTION

Packing in lattices is a geometric problem underlying error correction in many information transmission and storage systems. In the present paper we investigate packings in the A_n lattices endowed with the ℓ_1 metric, a problem arising naturally in several communication scenarios. The problem turns out to be closely related to some well-known combinatorial objects such as B_h sets and difference sets, and represents their geometric counterpart, in a sense made precise below.

The following subsection introduces A_n lattices and describes some of their properties that will be exploited later on. In Section 1.2 the motivation for this work is explained and several communication settings listed for which the results of the paper are relevant. In Sections 2–4 packings in A_n lattices are studied in more detail, and their connection with the notions of B_h sets and difference sets is demonstrated.

1.1. A_n lattice under ℓ_1 metric. The A_n lattice is defined as

$$(1.1) \quad A_n = \left\{ (x_0, x_1, \dots, x_n) : x_i \in \mathbb{Z}, \sum_{i=0}^n x_i = 0 \right\}$$

where \mathbb{Z} denotes the integers, as usual. A_1 is equivalent to \mathbb{Z} , A_2 to the hexagonal lattice, and A_3 to the face-centered cubic lattice (see [10]). The metric on A_n that we understand is essentially the ℓ_1 (also termed Manhattan or taxi) distance

$$(1.2) \quad d(\mathbf{x}, \mathbf{y}) = \frac{1}{2} \|\mathbf{x} - \mathbf{y}\|_1 = \frac{1}{2} \sum_{i=0}^n |x_i - y_i|,$$

Date: January 22, 2016.

2010 Mathematics Subject Classification. Primary: 05B10, 11B13, 11B75, 05B45, 94B25; Secondary: 52C22, 52C07, 52C17, 11H31, 68P30, 68R05.

Key words and phrases. B_h set, B_h sequence, Sidon set, difference set, prime power conjecture, A_n lattice, perfect code, tiling, group splitting, lattice packing, covering code, asymmetric channels.

Most of this work was done while the author was with the Department of Electrical Engineering, University of Novi Sad, Serbia. The work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia (grants TR32040 and III44003), and by the EU COST action IC1104.

where $\mathbf{x} = (x_0, x_1, \dots, x_n)$, $\mathbf{y} = (y_0, y_1, \dots, y_n)$; the constant $1/2$ is taken for convenience because $\|\mathbf{x} - \mathbf{y}\|_1$ is always even for $\mathbf{x}, \mathbf{y} \in A_n$. Distance d also represents the graph distance in A_n . Namely, if $\Gamma(A_n)$ is a graph with the vertex set A_n and with edges joining neighboring points (points at distance 1 under d), then $d(\mathbf{x}, \mathbf{y})$ is the length of the shortest path between \mathbf{x} and \mathbf{y} in $\Gamma(A_n)$.

Ball of radius 1 around $\mathbf{x} \in A_n$ contains $2\binom{n+1}{2} + 1 = n^2 + n + 1$ points of the form $\mathbf{x} + \mathbf{f}_{i,j}$, where $\mathbf{f}_{i,j}$ is a permutation of $(1, -1, 0, \dots, 0)$ having a 1 at the i 'th coordinate, a -1 at the j 'th coordinate, and zeros elsewhere (with the convention $\mathbf{f}_{i,i} = \mathbf{0}$). Convex interior of the points in the ball forms a highly symmetrical polytope having the following interesting property, among many others – the distance between any vertex and the center is equal to the distance between any two neighboring vertices. Ball of radius r around $\mathbf{x} \in A_n$ contains all the points with integral coordinates in the convex interior of $\{\mathbf{x} + r\mathbf{f}_{i,j}\}$.

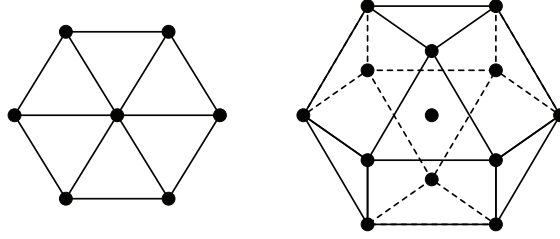


FIGURE 1. Ball of radius 1 in (A_2, d) – hexagon, and in (A_3, d) – cuboctahedron.

An error-correcting code of radius r in (A_n, d) (or any other discrete metric space for that matter), is a subset of A_n with the property that balls of radius r centered at points of this subset are disjoint. We say that a code is linear if it is a sublattice of A_n .

When studying packing problems, it is usually simpler to visualize \mathbb{Z}^n instead of an arbitrary lattice. In our case there is a trivial map that makes the transition to \mathbb{Z}^n and back very easy. For $\mathbf{x} = (x_1, \dots, x_n), \mathbf{y} = (y_1, \dots, y_n) \in \mathbb{Z}^n$, define the metric

$$(1.3) \quad d_a(\mathbf{x}, \mathbf{y}) = \max \left\{ \sum_{i: x_i > y_i} (x_i - y_i), \sum_{i: x_i < y_i} (y_i - x_i) \right\}.$$

This distance (restricted to $\{0, 1, \dots, q-1\}^n$) is used in the theory of codes for asymmetric channels [26, Ch. 2.3 and 9.1].

Lemma 1.1. (A_n, d) is isometric to (\mathbb{Z}^n, d_a) .

Proof. For $\mathbf{x} = (x_0, x_1, \dots, x_n)$, denote $\mathbf{x}' = (x_1, \dots, x_n)$. The map $\mathbf{x} \mapsto \mathbf{x}'$ is the desired isometry. Just observe that, for $\mathbf{x}, \mathbf{y} \in A_n$,

$$(1.4) \quad d(\mathbf{x}, \mathbf{y}) = \sum_{\substack{i=0 \\ x_i > y_i}}^n (x_i - y_i) = \sum_{\substack{i=0 \\ x_i < y_i}}^n (y_i - x_i)$$

because $\sum_{i=0}^n x_i = \sum_{i=0}^n y_i = 0$, and by examining the cases $x_0 \leq y_0$ it follows that

$$(1.5) \quad d(\mathbf{x}, \mathbf{y}) = \max \left\{ \sum_{\substack{i=1 \\ x_i > y_i}}^n (x_i - y_i), \sum_{\substack{i=1 \\ x_i < y_i}}^n (y_i - x_i) \right\} = d_a(\mathbf{x}', \mathbf{y}').$$

Furthermore, the map $\mathbf{x} \mapsto \mathbf{x}'$ is bijective. ■

Hence, packing and similar problems in (A_n, d) are equivalent¹ to those in (\mathbb{Z}^n, d_a) . Balls in (\mathbb{Z}^n, d_a) are “distorted” versions of the ones in (A_n, d) (see Fig. 5). For example, ball of radius r around $\mathbf{0}$ in (\mathbb{Z}^n, d_a) contains the points in \mathbb{Z}^n whose positive coordinates sum to at most r , and negative to at least $-r$.

We shall also need the following generalization of the ball in (\mathbb{Z}^n, d_a) :

$$(1.6) \quad S_n(r^+, r^-) = \left\{ \mathbf{x} \in \mathbb{Z}^n : \sum_{i: x_i > 0} x_i \leq r^+, \sum_{i: x_i < 0} |x_i| \leq r^- \right\},$$

where $r^+, r^- \geq 0$. Considering the symmetry of the shape $S_n(r^+, r^-)$ in the parameters r^+, r^- (see Fig. 2), we can assume that $r^- \leq r^+$. For $r^+ = r^- = r$, $S_n(r) \equiv S_n(r, r)$ is a ball of radius r around $\mathbf{0}$ in (\mathbb{Z}^n, d_a) .

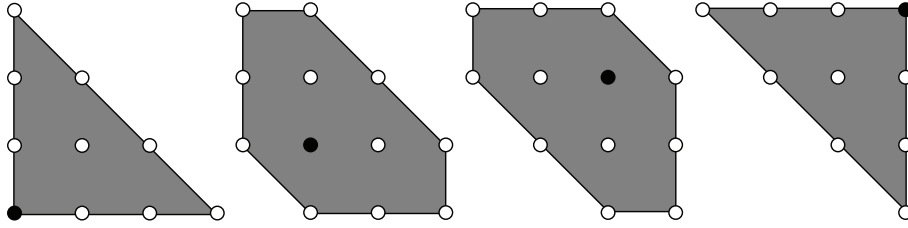


FIGURE 2. Shapes $S_2(r^+, r^-)$ for $r^+ + r^- = 3$. Black dot denotes the origin.

Lemma 1.2. *The cardinality of the set $S_n(r^+, r^-)$ is*

$$(1.7) \quad |S_n(r^+, r^-)| = \sum_{m=0}^{\min\{n, r^+\}} \binom{n}{m} \binom{r^+}{m} \binom{r^- + n - m}{n - m}.$$

Proof. Observe the vectors in $S_n(r^+, r^-)$ having m strictly positive coordinates, $m \in \{0, \dots, n\}$. These coordinates can be chosen in $\binom{n}{m}$ ways. For each choice, the “mass” $\leq r^+$ can be distributed over them in $\sum_{t=m}^{r^+} \binom{t-1}{m-1} = \binom{r^+}{m}$ ways (think of $t \leq r^+$ balls being placed into m bins, where at least one ball is required in each bin). Similarly, the mass $\leq r^-$ can be distributed over the remaining coordinates in $\sum_{t=0}^{r^-} \binom{t+n-m-1}{n-m-1} = \binom{r^-+n-m}{n-m}$ ways. ■

1.2. Motivation. Clearly, there can be no practical situation where the code space is infinite, but it is the underlying geometry of the problem that provides the motivation for studying codes in such spaces. In situations where the code space is, for example, a restriction of the A_n lattice, the corresponding restrictions of dense packings in (A_n, d) will most likely be good codes for the original problem. We list below several of the scenarios due to which it is worthwhile investigating the properties of codes in (A_n, d) , and describe each of them briefly.

1.2.1. Permutation channel. A permutation channel [28, 29]² over an alphabet \mathcal{Q} is a communication channel that takes sequences of symbols from \mathcal{Q} as inputs, and for any input sequence outputs a random permutation of this sequence. This channel is intended to model packet networks based on routing in which the receiver cannot rely on the packets

¹This fact is mentioned in [14] for the case $n = 2$, though the interpretation via the metric d_a is not given.

²Other approaches to coding for random permutations [36, 15] should also be mentioned here. However, they are all essentially special cases of the “multiset” framework in [28, 29]. This framework is the most general one for the permutation channel, and enables the construction of the largest codes with given parameters. Coding for limited permutations/transpositions has also been addressed in the literature [39, 30].

being delivered in any particular order, as well as several other communication scenarios where a similar effect occurs, such as systems for distributed storage, data gathering in wireless sensor networks, etc.

It was shown in [28] that the appropriate space for defining error-correcting codes for such channels is³ (Δ_ℓ^n, d) , where

$$(1.8) \quad \Delta_\ell^n = \left\{ (x_0, x_1, \dots, x_n) \in \mathbb{Z}_{\geq 0}^{n+1} : \sum_{i=0}^n x_i = \ell \right\}$$

is the discrete standard simplex, and d is the metric given by (1.2). Notice that Δ_ℓ^n is just the translated A_n lattice restricted to the nonnegative orthant. This restriction is the reason that this space lacks some nice properties that are usually exploited when studying bounds on codes, packing problems, and the like. In order to study the underlying geometric problem, one can disregard these restrictions and investigate the corresponding problems in (A_n, d) . The same approach is employed for some other types of codes; see for example [7, 8, 40] where certain packing problems in \mathbb{Z}^n are studied, with applications to codes for flash memories.

1.2.2. 0-Insertion/Deletion Channel. As another example observe the binary channel in which insertions and/or deletions of the symbol 0 are the only possible impairments [32]. Insertions and deletions in strings of symbols can be caused by synchronization errors, and we are now assuming that only one of the two binary symbols is susceptible to such errors, perhaps due to their different physical representations.

A very natural way of communication that can maintain codeword-level synchronization is to use a constant-weight code of length n and Hamming weight w , and put an additional 1 at the end of each codeword (this 1 acts as a delimiter between successively sent codewords). Even though the length of each codeword can change, the receiver can easily find the beginning and the end of each by counting the 1's, which are unaffected by the channel. Note that such codewords can be represented as $(w+1)$ -tuples of nonnegative integers (x_0, \dots, x_w) summing to $n-w$, where x_i is the number of zeros between the i 'th and the $(i+1)$ 'th one. This means that the code space just described is equivalent to Δ_{n-w}^w .

Furthermore, the distance between binary strings of weight w that is suitable in this scenario is the smallest number of insertions and/or deletions of zeros that can transform one of the strings to the other. This is a variation of the Levenshtein distance appropriate for the channel treated here, and it is in fact equal to the ℓ_1 distance between the integer representations of the sequences as described above. Therefore, we again have the restriction of (A_n, d) as a code space in question.

1.2.3. Asymmetric channels. Observe the channel with input alphabet $\mathcal{Q} = \{0, 1, \dots, q-1\}$ in which the transmitted symbols can be increased, decreased, or remain intact (we are not concerned here with a detailed description of the channel, but wish to make a rather general point). The symbols in \mathcal{Q} can be thought of as voltage levels, e.g., in baseband digital signal transmission, or in multi-level flash memory [8, 40].

In some situations, it may be desirable to treat the two types of errors separately when designing an error-correcting code, and to impose different bounds on the number of “up” and “down” errors that can be corrected. This is because these types of errors can be of different nature and/or different origin, and the probabilities of a symbol being increased/decreased might be different. Namely, suppose that we want to guarantee that all patterns of $\leq r^+$ “up” and $\leq r^-$ “down” errors can be corrected at the receiving side.

³The appropriate space is in fact $\mathbb{Z}_{\geq 0}^{n+1}$, where $n+1 = |\mathcal{Q}|$. However, if the cardinality of each multi-set/codeword is fixed to ℓ , then Δ_ℓ^n is obtained [29]. This assumption is quite natural, and also simplifies the decoding.

This will be achieved if and only if the translates of the set $S_n(r^+, r^-)$ by the codewords are disjoint. In other words, the decoding regions are defined precisely by the set $S_n(r^+, r^-)$, and hence, packing problems in (\mathbb{Z}^n, d_a) are relevant for studying and designing good codes in this case, at least for large q .

To be a little more concrete, consider also the following channel model. The transmitter sends x_i particles (or packets) in the i 'th time slot. The particles are assumed identical, implying that the transmitted sequence can be identified with a sequence of nonnegative integers $(x_1, \dots, x_n) \in \mathbb{Z}_{\geq 0}^n$. In the channel, some of the particles can be lost (deletions), while new particles can appear from the surrounding medium (insertions). Additionally, one can also allow delays of the particles in the model [27] (a delay can be thought of as a deletion followed by an insertion several time slots later). Such channels are of interest in molecular communications, discrete-time queuing systems, etc. If we wish to guarantee that all patterns of $\leq r^+$ insertions and $\leq r^-$ deletions of particles are correctable, we need to make sure that the translates of $S_n(r^+, r^-)$ are disjoint.

2. LINEAR CODES IN A_n LATTICES AND B_h SETS

In this section, linear codes in (A_n, d) and, more generally, lattice packings of the shape $S_n(r^+, r^-)$ in \mathbb{Z}^n , are studied. The connection to so-called B_h sets is described, and bounds on the packing radius r and the dimension n derived.

2.1. B_h sets. Let G be an Abelian group⁴ of order v , written additively. A set $B = \{b_0, b_1, \dots, b_{k-1}\} \subseteq G$ is said to be a B_h set (or B_h sequence, or *Sidon set* of order h) if the sums $b_{i_1} + \dots + b_{i_h}$, $0 \leq i_1 \leq \dots \leq i_h \leq k-1$, are all different. B_2 sets were introduced by Sidon⁵ [41], and a construction of optimal such sets in $\mathbb{Z}_v \equiv \mathbb{Z}/v\mathbb{Z}$ was given by Singer [42] for $k-1$ a prime power and $v = k^2 - k + 1$. Bose and Chowla [6] gave a construction of B_h sets in \mathbb{Z}_v for arbitrary $h \geq 1$ when: 1) k is a prime power and $v = k^h - 1$, and 2) $n = k-1$ is a prime power and $v = (n^{h+1} - 1)/(n - 1)$. Since these pioneering papers, research in this area of combinatorial number theory has been extensive, see [38] for references. It has also found several applications in coding theory, see, e.g., [4, 12, 18, 48].

As indicated above, $k = n+1$ will denote the size of the B_h set in question. Note that if $\{b_0, b_1, \dots, b_n\}$ is a B_h set, then so is $\{0, b_1 - b_0, \dots, b_n - b_0\}$, and vice versa; we shall therefore assume in the sequel that $b_0 = 0$. With this convention we have that all the sums $b_{i_1} + \dots + b_{i_u}$, for arbitrary $0 \leq u \leq h$ and $1 \leq i_1 \leq \dots \leq i_u \leq n$, are different.

2.2. B_h sets and packings in (\mathbb{Z}^n, d_a) . If $S, \mathcal{L} \subseteq \mathbb{Z}^n$, \mathcal{L} a lattice, we say that S packs \mathbb{Z}^n with lattice \mathcal{L} if the translates $S + \mathbf{x}$ and $S + \mathbf{y}$ are disjoint for every $\mathbf{x}, \mathbf{y} \in \mathcal{L}$, $\mathbf{x} \neq \mathbf{y}$. In particular, we are interested in packings by the shape $S_n(r^+, r^-)$ defined in (1.6). In this terminology, a linear code of radius r is a lattice packing by the balls $S_n(r, r)$. The following theorem states that such packings are, in a sense, geometric realizations of B_h sets.

Theorem 2.1. *Let $h \geq 1$ and $r^+, r^- \geq 0$ be integers satisfying $r^+ + r^- = h$.*

(a) *Assume that $B = \{0, b_1, \dots, b_n\}$ is a B_h set in an Abelian group G of order v , and that B generates G . Then $S_n(r^+, r^-)$ packs \mathbb{Z}^n with lattice*

$$(2.1) \quad \mathcal{L} = \left\{ \mathbf{x} \in \mathbb{Z}^n : \sum_{i=1}^n x_i b_i = 0 \right\},$$

and G is isomorphic to \mathbb{Z}^n/\mathcal{L} (here $x_i b_i$ denotes the sum in G of $|x_i|$ copies of b_i if $x_i > 0$, and of $-b_i$ if $x_i < 0$).

⁴Only Abelian groups are treated in the paper, this is understood even if not explicitly stated.

⁵Though there were some earlier appearances of the problem, see [38].

(b) Conversely, if $S_n(r^+, r^-)$ packs \mathbb{Z}^n with lattice \mathcal{L}' , then the group $G = \mathbb{Z}^n / \mathcal{L}'$ contains a B_h set of cardinality $n + 1$ that generates G .

Proof. The claim is an instance of the familiar group-theoretic formulation of lattice packing/tiling problems [43, 20, 44, 16, 21, 46] (the formulation in [45] is the one we used here). In coding theoretic terms, the condition that the translates of $S_n(r^+, r^-)$ are disjoint means that the error-vectors from $S_n(r^+, r^-)$ are correctable and have different syndromes. Since positive coordinates of these vectors sum to $t \leq r^+$ and negative to $-s \geq -r^-$, we see from (2.1) that the syndromes are of the form $b_{i_1} + \dots + b_{i_t} - b_{j_1} - \dots - b_{j_s}$. Now just observe that all the sums $b_{i_1} + \dots + b_{i_u}$ are different, where u goes through $\{0, 1, \dots, h\}$ and $1 \leq i_1 \leq \dots \leq i_u \leq n$, if and only if all linear combinations of the form $b_{i_1} + \dots + b_{i_t} - b_{j_1} - \dots - b_{j_s}$ are different, where t goes through $\{0, 1, \dots, r^+\}$, s through $\{0, 1, \dots, r^-\}$, and $1 \leq i_1 \leq \dots \leq i_t \leq n$, $1 \leq j_1 \leq \dots \leq j_s \leq n$. Hence the need for a B_h set. \blacksquare

In other words, the code (2.1) defined by a $B_{r^++r^-}$ set with $n + 1$ elements is capable of correcting all error-vectors from the set $S_n(r^+, r^-)$, and the size of the Voronoi region of an arbitrary codeword is v . In particular, B_{2r} sets correspond in a direct way to error-correcting codes of radius r in (\mathbb{Z}^n, d_a) , or equivalently in (A_n, d) . Note also that the packing lattice \mathcal{L} does not depend on the particular values of r^+, r^- , but only on their sum. However, the cardinality of the “decoding region” $S_n(r^+, r^-)$ varies with r^+ , and so does the packing density (the fraction of the space covered) $\frac{1}{v}|S_n(r^+, r^-)|$.

Example 1. The set $\{(0, 0), (1, 1), (0, 5)\} \subseteq \mathbb{Z}_2 \times \mathbb{Z}_6$ is a B_3 set. The corresponding packing of \mathbb{Z}^2 is illustrated in Figure 3. It is in fact a perfect packing, i.e., a tiling; this will be further discussed in Section 3. \triangle

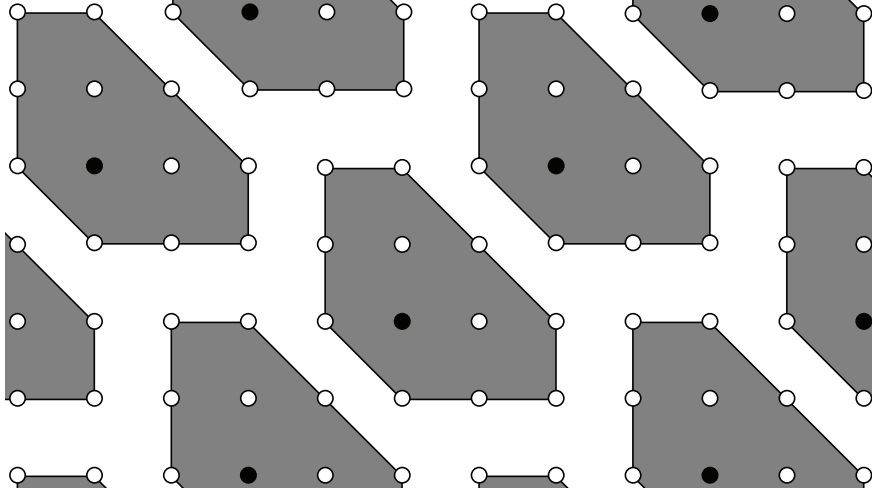


FIGURE 3. Tiling of \mathbb{Z}^2 by the shape $S_2(2, 1)$.

2.3. Bounds on the packing radius r and the dimension n . We now make several simple observations about the density of the lattice packings in (\mathbb{Z}^n, d_a) , and derive bounds on r and n . For easier comparison with the known bounds, we shall state them in terms of the parameters of B_h sets. Recalling that the dimension of the space n corresponds to the cardinality of the B_h set k ($k = n + 1$), and the radius of the code r to the parameter h ($h = 2r$), one can easily restate the bounds in terms of these geometric quantities.

A major part of research on B_h sets is concentrated on determining extremal size of such sets for given h, v , or the asymptotic behavior of k for given h and for $v \rightarrow \infty$. Despite a

large amount of work, however, determining tight bounds remains an open problem. Let $f_h(v)$ denote the size of the largest B_h set in *all* Abelian groups of order v , $h_k(v)$ the largest h for which there is a B_h set of size k in some Abelian group of order v , and $\phi(h, k)$ the order of the smallest Abelian group containing some B_h set of size k . This notation is from [24], except the functions are defined to include all finite Abelian groups, rather than just the cyclic ones. The following bounds are currently the best known [24, 9]:

For any fixed $h \geq 1$,

$$(2.2) \quad \phi(h, k) \geq \frac{k^h}{\lceil h/2 \rceil! \lfloor h/2 \rfloor!} + o(k^h)$$

and

$$(2.3) \quad f_h(v) \leq v^{\frac{1}{h}} \cdot (\lfloor h/2 \rfloor! \lceil h/2 \rceil!)^{\frac{1}{h}} + O(1),$$

and for any fixed $k = n + 1 \geq 2$,

$$(2.4) \quad v^{\frac{1}{n}} - 2 < h_k(v) \leq v^{\frac{1}{n}} (n!)^{\frac{1}{n}}.$$

We illustrate next how nontrivial bounds can be derived in a straightforward way using Theorem 2.1.

Theorem 2.2. *For all $h \geq 1$ and $k \geq \lceil h/2 \rceil$,*

$$(2.5) \quad \phi(h, k) > \frac{(k - \lceil h/2 \rceil)^h}{\lceil h/2 \rceil! \lfloor h/2 \rfloor!}.$$

For all $h \geq 1$ and $v \geq 2$,

$$(2.6) \quad f_h(v) < v^{\frac{1}{h}} \cdot (\lfloor h/2 \rfloor! \lceil h/2 \rceil!)^{\frac{1}{h}} + \lceil h/2 \rceil.$$

For all $k = n + 1 \geq 2$ and $h \geq 2k - 4$,

$$(2.7) \quad \phi(h, k) > \frac{(h - 2n + 2)^n}{n!} \frac{\binom{2n}{n}}{2^n}.$$

For all $k = n + 1 \geq 2$ and $v \geq 2$,

$$(2.8) \quad h_k(v) < v^{\frac{1}{n}} \cdot 2 \left((n!)^3 / (2n)! \right)^{\frac{1}{n}} + 2n - 2.$$

Proof. Suppose that $\{0, b_1, \dots, b_n\}$ is a B_h set in a group G of order v , and \mathcal{L} the corresponding lattice, see (2.1). By Theorem 2.1, $G \cong \mathbb{Z}^n / \mathcal{L}$ and the translations of the shape $S_n(r^+, r^-)$ by vectors in \mathcal{L} are disjoint. Therefore, for $n \geq r^+$,

$$(2.9) \quad \begin{aligned} v &\geq |S_n(r^+, r^-)| \\ &= \sum_{m=0}^{r^+} \binom{n}{m} \binom{r^+}{m} \binom{r^- + n - m}{n - m} \\ &\geq \sum_{m=0}^{r^+} \frac{(n - m + 1)^m}{m!} \binom{r^+}{m} \frac{(n - m + 1)^{r^-}}{r^-!} \\ &> \frac{(n - r^+ + 1)^h}{r^+! r^-!}, \end{aligned}$$

where we used $\binom{n}{m} \geq \frac{(n - m + 1)^m}{m!}$, and the last inequality is obtained by keeping only the summand $m = r^+$. This implies (2.5) and (2.6) by taking $r^+ = \lceil h/2 \rceil$ (this choice

minimizes the denominator $r^+!r^-!$).

Similarly, if we let $0 \leq r^+ - n \leq r^-$, then

$$\begin{aligned}
 (2.10) \quad v &\geq |S_n(r^+, r^-)| \\
 &= \sum_{m=0}^n \binom{n}{m} \binom{r^+}{m} \binom{r^- + n - m}{n - m} \\
 &\geq \sum_{m=0}^n \binom{n}{m} \frac{(r^+ - m + 1)^m}{m!} \frac{(r^- + 1)^{(n-m)}}{(n-m)!} \\
 &= \frac{1}{n!} \sum_{m=0}^n \binom{n}{m}^2 (r^+ - m + 1)^m (r^- + 1)^{(n-m)} \\
 &> \frac{(r^+ - n + 1)^n}{n!} \binom{2n}{n}.
 \end{aligned}$$

In the last step we used the assumption $r^- \geq r^+ - n$ and the identity $\sum_{m=0}^n \binom{n}{m}^2 = \binom{2n}{n}$. When $r^+ = \lceil h/2 \rceil$ we get (2.7) and (2.8). \blacksquare

The above derivations, apart from being simple, have the advantage of including all finite Abelian groups. The bounds in (2.5) and (2.6) are the same as the known bounds (2.2) and (2.3), but with explicit error terms, while the bounds (2.7) and (2.8) improve on the known bounds by a factor of $2^{-n} \binom{2n}{n} > 1$, $n > 1$. The lower bound in (2.4) can also be derived by an easy geometric argument. Namely, since the body $S_n(r^+, r^-)$ is contained in a hypercube $\{-r^-, \dots, 0, \dots, r^+\}^n$ of size $(h+1)^n$, and since this hypercube tiles \mathbb{Z}^n , we conclude that

$$(2.11) \quad \phi(h, k) \leq (h+1)^n,$$

which gives the desired bound.

Another important quantity to be mentioned, measuring the quality of the code, is the packing density. Let $\mu_n(r)$ be the largest density of all linear codes of radius r in (A_n, d) . Then the above bounds imply that

$$(2.12) \quad \frac{1}{(r!)^2} \leq \limsup_{n \rightarrow \infty} \mu_n(r) \leq 1,$$

and

$$(2.13) \quad \frac{(2n)!}{(n!)^3 2^n} \leq \limsup_{r \rightarrow \infty} \mu_n(r) \leq 1.$$

The left-hand inequality in (2.12) follows from the construction of Bose and Chowla [6] which implies that $\phi(h, k) < k^h$ when k is a prime power. In section 3.2 we shall in fact prove that, for every $n \geq 3$,

$$(2.14) \quad \limsup_{r \rightarrow \infty} \mu_n(r) < 1.$$

The consequence of this is that, for every $n \geq 3$, there exists a constant $c_n > 1$ such that

$$(2.15) \quad \phi(h, k) > \frac{h^n}{n!} \frac{\binom{2n}{n}}{2^n} c_n + o(h^n),$$

further improving on the bounds in (2.7) and (2.8).

3. PERFECT CODES IN (A_n, d)

A code in a given discrete metric space is said to be *r-perfect* if balls of radius r around the codewords are disjoint and cover the entire space. Geometrically speaking, these are the best packings that one can have; their packing density is equal to 1 – the largest possible value. It is therefore important to study their existence, and methods of construction when they do exist. Notice that, by Theorem 2.1, linear r -perfect codes in (A_n, d) correspond to B_{2r} sets of cardinality $n + 1$ in an Abelian group of order $v = |S_n(r)|$.

Perfect codes are also studied in graph theory as one of the several variants of dominating sets [3, 25] (see also [34]).

3.1. 1-Perfect codes and planar difference sets. Linear 1-perfect codes in (A_n, d) correspond to B_2 sets (Sidon sets) of cardinality $k = n + 1$ in an Abelian group G of order $v = n^2 + n + 1$. Such sets are better known in the literature as *planar* (or *simple*) *difference sets*. Notice that all the sums $b_i + b_j$ are different, up to the order of the summands, if and only if all the differences $b_i - b_j$ for $i \neq j$ are different. The additional requirement for difference sets, compared to B_2 sets, is that every nonzero element of the group can be expressed as such a difference, which is equivalent to saying that the order of the group is $v = k(k - 1) + 1 = n^2 + n + 1$. The *order* of a planar difference set D of size $k = n + 1$ is defined as $k - 1 = n$. If G is Abelian, cyclic, etc., then D is also said to be Abelian, cyclic, etc., respectively.

Planar difference sets and their generalizations (see Section 4) are very well-studied, and a large body of literature is devoted to the investigation of their properties [5]. One of the most familiar problems in the area concerning the existence of these objects for specific sets of parameters is the so-called *prime power conjecture* [5, Conj. 7.5, p. 346]: Planar difference set of order n exists if and only if n is a prime power (counting $n = 1$ as a prime power). Existence of such sets for $n = p^m$, p prime, $m \in \mathbb{Z}_{\geq 0}$, was demonstrated by Singer [42], but the necessity of this condition remains an open problem for nearly eight decades. Difference sets have also been applied in communications and coding theory in various settings, see for example [13, 1, 31].

The following claim is a slight modification of Theorem 2.1.

Theorem 3.1. *There exists an Abelian planar difference set of order n if and only if the space (A_n, d) admits a linear 1-perfect code.* ■

Existence of such codes when n is a prime power follows from the existence of the corresponding difference sets [42], but the necessity of this condition is open and is equivalent to the prime power conjecture.

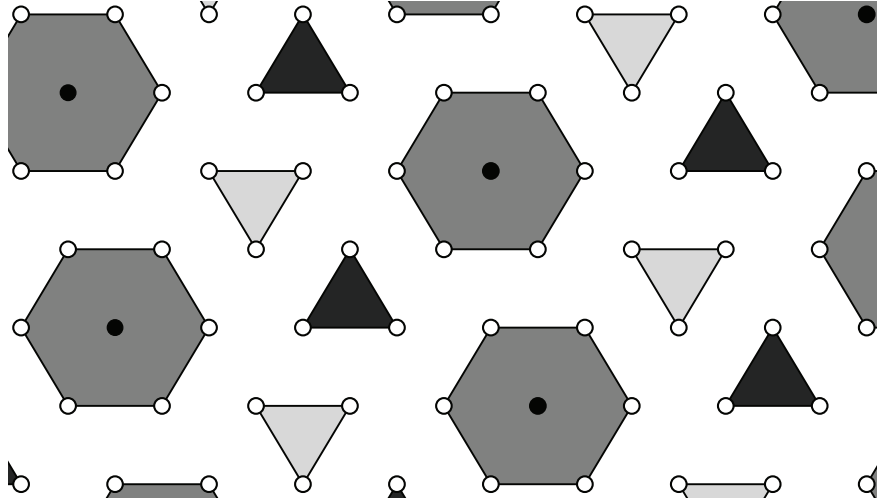
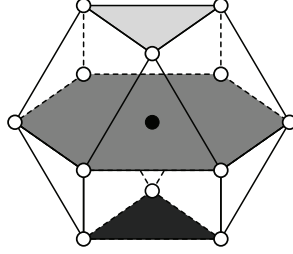
Conjecture 3.2 (Prime power conjecture). *There exists a linear 1-perfect code in (A_n, d) (or, equivalently, in (\mathbb{Z}^n, d_a)) if and only if n is a prime power.* △

A stronger conjecture would claim the above even for nonlinear codes.

Example 2. Consider a planar difference set $D = \{0, 1, 3, 9\} \subset \mathbb{Z}_{13}$. The corresponding 1-perfect code in (A_3, d) is illustrated in Fig. 4(a). The figure shows the intersection of A_3 with the plane $x_0 = 0$; the intersections of a ball of radius 1 in A_3 with the planes $x_0 = \text{const}$ are shown in Fig. 4(b) for clarification. △

Another important unsolved problem in the field is the following: All Abelian planar difference sets live in cyclic groups [5, Conj. 7.7, p. 346]. Since the group G containing the difference set which defines the code \mathcal{L} is isomorphic to A_n/\mathcal{L} , the statement that G is cyclic, i.e., that it has a generator, is equivalent to the following:

Conjecture 3.3 (All Abelian planar difference sets are cyclic). *Let \mathcal{L} be a linear 1-perfect code in (A_n, d) . Then the period of \mathcal{L} in A_n along the direction $\mathbf{f}_{i,j}$ is equal to $n^2 + n + 1$ for at least one vector $\mathbf{f}_{i,j}$, $(i, j) \in \{0, 1, \dots, n\}^2$.* △

(a) The code viewed in the plane $x_0 = 0$.(b) Intersections of a ball in (A_3, d) with the planes $x_0 = \text{const.}$ FIGURE 4. 1-perfect code in (A_3, d) .

The cyclic case. In the rest of this subsection we restrict our attention to cyclic planar difference sets of order n , i.e., it is assumed that the group we are working with is \mathbb{Z}_v , $v = n^2 + n + 1$; as mentioned above, this in fact might not be a restriction at all. So let $D = \{d_0, d_1, \dots, d_n\} \subset \mathbb{Z}_v$ be a difference set and \mathcal{L} the corresponding code (see (2.1)).

We shall assume that $d_0 = 0$, $d_1 = 1$. (This is not a loss in generality because if D is a difference set, there exist two elements, say $d_0, d_1 \in D$, such that $d_1 - d_0 = 1$. Then we can take the equivalent difference set $D' = \{d_i - d_0 : d_i \in D\}$ which obviously contains 0 and 1.) In this case the generator matrix of the code (lattice) \mathcal{L} has the following form

$$(3.1) \quad B(\mathcal{L}) = \begin{pmatrix} v & 0 & 0 & \cdots & 0 \\ -d_2 & 1 & 0 & \cdots & 0 \\ -d_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -d_n & 0 & 0 & \cdots & 1 \end{pmatrix},$$

i.e., the codewords are the vectors $\mathbf{x} = \boldsymbol{\xi} \cdot B(\mathcal{L})$, $\boldsymbol{\xi} \in \mathbb{Z}^n$ (the vectors are written as rows). The generator matrix of the dual lattice \mathcal{L}^* is

$$(3.2) \quad B(\mathcal{L}^*) = B(\mathcal{L})^{-T} = \begin{pmatrix} \frac{1}{v} & \frac{d_2}{v} & \frac{d_3}{v} & \cdots & \frac{d_n}{v} \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

We have disregarded above the 0-coordinate because $d_0 = 0$. Therefore, $B(\mathcal{L})$ is in fact a generator matrix of the corresponding code in (\mathbb{Z}^n, d_a) (see Lemma 1.1).

Finite alphabet. By taking the codewords of \mathcal{L} modulo $v = n^2 + n + 1$, one obtains a finite code in \mathbb{Z}_v^n defined by the generator matrix (over \mathbb{Z}_v)

$$(3.3) \quad \begin{pmatrix} -d_2 & 1 & 0 & \cdots & 0 \\ -d_3 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -d_n & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

This code is of length n , has v^{n-1} codewords, and is 1-perfect (under the obvious “modulo v version” of the d_a metric). It is also systematic, i.e., the information sequence itself is a part of the codeword. The “parity check” matrix of the code is $H = (1 \ d_2 \ \cdots \ d_n)$. Thus, the codewords are all those vectors $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}_v^n$ for which $H \cdot \mathbf{x}^T = 0 \pmod v$, and the syndromes of the correctable error vectors $\mathbf{f}_{i,j}$ (with the 0-coordinate left out) are $H \cdot \mathbf{f}_{i,j}^T = d_i - d_j$.

3.2. r -perfect codes in (A_n, d) . It can be verified directly that, in dimensions one and two, r -perfect codes exist for any r ; the corresponding B_{2r} sets might therefore be called *perfect B_{2r} sets*. In higher dimensions, however, it does not seem possible to tile (A_n, d) by balls of radius $r > 1$. We shall not be able to prove this claim here, but Theorem 3.5 below is a step in this direction.

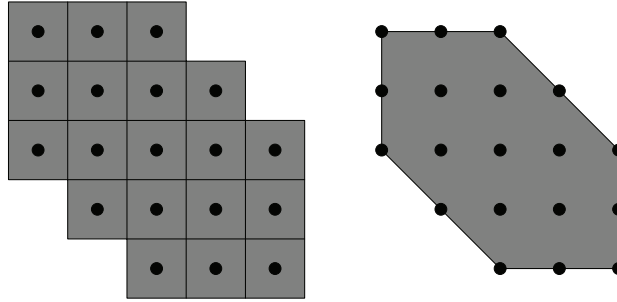


FIGURE 5. Bodies in \mathbb{R}^2 corresponding to a ball of radius 2 in (\mathbb{Z}^2, d_a) : The cubical tile (left) and the convex interior (right).

Let $S_n(r) \equiv S_n(r, r)$ be the ball of radius r around $\mathbf{0}$ in (\mathbb{Z}^n, d_a) . Let $D_n(r)$ be the body in \mathbb{R}^n defined as the union of unit cubes translated to the points of $S_n(r)$, namely, $D_n(r) = \bigcup_{\mathbf{y} \in S_n(r)} (\mathbf{y} + [-1/2, 1/2]^n)$, and $C_n(r)$ the body defined as the convex interior in \mathbb{R}^n of the points in $S_n(r)$ (see Fig. 5).

Lemma 3.4. *The volumes of the bodies $D_n(r)$ and $C_n(r)$ are given by*

$$(3.4) \quad \text{Vol}(D_n(r)) = \sum_{m=0}^{\min\{n, r\}} \binom{n}{m} \binom{r}{m} \binom{r+n-m}{n-m}$$

$$(3.5) \quad \text{Vol}(C_n(r)) = \frac{r^n}{n!} \binom{2n}{n},$$

and they satisfy $\lim_{r \rightarrow \infty} \text{Vol}(C_n(r)) / \text{Vol}(D_n(r)) = 1$.

Proof. Since $D_n(r)$ consists of unit cubes, its volume is $\text{Vol}(D_n(r)) = |S_n(r)|$, which gives the above expression by Lemma 1.2.

To compute the volume of $C_n(r)$, observe its intersection with the orthant $x_1, \dots, x_m > 0$, $x_{m+1}, \dots, x_n \leq 0$, where $m \in \{0, \dots, n\}$. The volume of this intersection is the product

of the volumes of the m -simplex $\{(x_1, \dots, x_m) : x_i > 0, \sum x_i \leq r\}$, which is known to be $r^m/m!$, and of the $(n-m)$ -simplex $\{(x_{m+1}, \dots, x_n) : x_i \leq 0, \sum x_i \geq -r\}$, which is $r^{n-m}/(n-m)!$. This implies that $\text{Vol}(C_n(r)) = \sum_{m=0}^n \binom{n}{m} \frac{r^m}{m!} \frac{r^{n-m}}{(n-m)!}$, which is equivalent to (3.5) since $\sum_{m=0}^n \binom{n}{m}^2 = \binom{2n}{n}$.

To prove the third claim observe that if $r \rightarrow \infty$, then $\binom{r}{m} \sim \frac{r^m}{m!}$ and so $\text{Vol}(D_n(r)) \sim \frac{r^n}{n!} \binom{2n}{n}$. ■

Theorem 3.5. *There are no r -perfect codes in (A_n, d) , $n \geq 3$, for large enough r , i.e., for $r \geq r_0(n)$.*

Proof. The proof is based on the same idea as the one for r -perfect codes in \mathbb{Z}^n under ℓ_1 distance [17]. First observe that an r -perfect code in (\mathbb{Z}^n, d_a) would induce a tiling of \mathbb{R}^n by $D_n(r)$, and a packing by $C_n(r)$. The relative efficiency of the latter with respect to the former is defined as the ratio of the volumes of these bodies, $\text{Vol}(C_n(r))/\text{Vol}(D_n(r))$, which by Lemma 3.4 tends to 1 as r grows indefinitely. This has the following consequence: If an r -perfect code exists in (\mathbb{Z}^n, d_a) for arbitrarily large r , then there exists a tiling of \mathbb{R}^n by translates of $D_n(r)$ for arbitrarily large r , which further implies that a packing of \mathbb{R}^n by translates of $C_n(r)$ exists which has efficiency arbitrarily close to 1. But then there would also be a packing by $C_n(r)$ of efficiency 1, i.e., a tiling (in [17, Appendix] it is shown that there exists a packing whose density is the supremum of the densities of all possible packings with a given body). This is a contradiction. Namely, Minkowski [37] (see also [35, Thm 1]) has shown that a necessary condition for a convex body to be able to tile space is that it be a polytope with centrally symmetric⁶ facets, which $C_n(r)$ fails to satisfy for $n \geq 3$. For example, the facet which is the intersection of $C_n(r)$ with the hyperplane $x_1 = -r$ is the simplex $\{(x_2, \dots, x_n) : x_i \geq 0, \sum_{i=2}^n x_i \leq r\}$, a non-centrally-symmetric body. ■

In summary, we have shown that linear r -perfect codes in (A_n, d) exist for:

- $n \in \{1, 2\}$, r arbitrary,
- $n \geq 3$ a prime power, $r = 1$.

The statement that these are the only cases (apart from the trivial one $r = 0$), even if nonlinear codes are allowed, is a further strengthening of the prime power conjecture. It should also be contrasted with the Golomb-Welch conjecture [17] (see also, e.g., [22, 23]) stating that r -perfect codes in \mathbb{Z}^n under ℓ_1 metric exist only in the following cases: 1) $n \in \{1, 2\}$, r arbitrary, and 2) $r = 1$, n arbitrary.

Remark 3.6. The same argument as the one in the previous proof shows that the packing density (for general packings, not necessarily lattices) of a code in (\mathbb{Z}^n, d_a) is bounded away from one as $r \rightarrow \infty$. This implies (2.14) and, as commented at the end of Section 2.3, gives an improvement of the bounds on $\phi(h, k)$ and $h_k(v)$. Δ

3.3. Tilings by $S_n(r+1, r)$. One could also define perfect B_{2r+1} sets as those that give rise to tilings by the shapes $S_n(r+1, r)$. In dimension 1 the problem is trivial, and in dimension 2 the tilings exist for any $r \geq 0$ (see Fig. 3). The tiling lattice \mathcal{L} for the shape $S_2(r+1, r)$ is the one spanned by the vectors $(r+1, r+1)$ and $(0, 3r+3)$, and it is unique, which can be seen from the figure. It should be noted that, for $r \geq 1$, \mathbb{Z}^2/\mathcal{L} is not cyclic and hence, perfect B_{2r+1} sets of size 3 do not exist in cyclic groups. For $r = 0$, tiling of \mathbb{Z}^n by $S_n(1, 0)$ exists for any n ; it corresponds to the trivial B_1 set G in an arbitrary Abelian group G .

In dimensions $n \geq 3$, a statement analogous to Theorem 3.5 can be proven to exclude such tilings for r large enough.

⁶A polytope $P \subset \mathbb{R}^n$ is centrally symmetric if its translation $\tilde{P} = P - \mathbf{x}$ satisfies $\tilde{P} = -\tilde{P}$ for some $\mathbf{x} \in \mathbb{R}^n$.

4. (v, k, λ) -DIFFERENCE SETS AND COVERINGS OF A_n

There are several generalizations of difference sets and B_h sets which can be interpreted geometrically using the same methods as above. We mention here one such extensively studied notion [5], that of a (v, k, λ) -difference set, which generalizes planar difference sets studied in the previous section. Let G be a group of order v , as before. A set $D \subseteq G$ of size k is said to be a (v, k, λ) -*difference set* if every nonzero element of G can be expressed as a difference $d_i - d_j$ of two elements from D in exactly λ ways. The parameters v, k, λ then necessarily satisfy the identity $\lambda(v - 1) = k(k - 1)$. The *order* of such a difference set is defined as $k - \lambda$. Planar difference sets are obtained for $\lambda = 1$.

Geometry of Abelian (v, k, λ) -difference sets. In the following, when using concepts from graph theory in our setting, we have in mind the graph representation $\Gamma(A_n)$ of A_n , as introduced in Section 1.1. An (r, i, j) -cover (or (r, i, j) -covering code) in a graph $\Gamma = (V, E)$ [2] is a set of its vertices $S \subseteq V$ with the property that every element of S is covered by exactly i balls of radius r centered at elements of S , while every element of $V \setminus S$ is covered by exactly j such balls. Special cases of such sets, namely $(1, i, j)$ -covers, have also been studied in the context of domination theory in graphs [47]; in coding theory, $(r, 1, 1)$ -covers are r -perfect codes. An independent set in a graph $\Gamma = (V, E)$ is a subset of its vertices $I \subseteq V$, no two of which are adjacent in Γ .

The proof of the following theorem is an easy generalization of the connection between lattice tilings and group splitting used in the previous sections [43, 20, 44, 16, 21] (see also [46]). We write it nonetheless for completeness.

Theorem 4.1. *There exists an Abelian $(v, n + 1, \lambda)$ -difference set if and only if the lattice A_n contains a $(1, 1, \lambda)$ -covering sublattice.*

Proof. Suppose that $D = \{d_0, d_1, \dots, d_n\}$ is a $(v, n + 1, \lambda)$ -difference set in an Abelian group G , and observe the sublattice

$$(4.1) \quad \mathcal{L} = \left\{ \mathbf{x} \in A_n : \sum_{i=0}^n x_i d_i = 0 \right\}.$$

\mathcal{L} is a $(1, 1, \lambda)$ -cover in A_n . To see this, consider a point $\mathbf{y} = (y_0, y_1, \dots, y_n) \notin \mathcal{L}$, meaning that $\sum_{i=0}^n y_i d_i = a \in G$, $a \neq 0$. The neighbors of \mathbf{y} are of the form $\mathbf{y} + \mathbf{f}_{i,j}$, $i \neq j$. Since D is a difference set, $-a \in G$ can be written as a difference of the elements from D in exactly λ ways, meaning that there are λ different pairs (s, t) for which $d_s - d_t = -a$, $d_s, d_t \in D$. For every such pair observe the point $\mathbf{z}_{s,t} = \mathbf{y} + \mathbf{f}_{s,t}$. $\mathbf{z}_{s,t} \in \mathcal{L}$ because $\sum_{i=0}^n z_i d_i = \sum_{i=0}^n y_i d_i + d_s - d_t = a - a = 0$. Therefore, there are exactly λ points in the lattice \mathcal{L} that are adjacent to \mathbf{y} , i.e., such that balls of radius 1 around them cover \mathbf{y} . To show that the elements of \mathcal{L} are covered only by the balls around themselves (i.e., that \mathcal{L} is an independent set in $\Gamma(A_n)$), observe that if there were two points at distance 1 in \mathcal{L} , then by the same argument as above we would obtain that $d_s - d_t = 0$, i.e., $d_s = d_t$ for some $s \neq t$, which is not possible if $|D| = n + 1$.

For the other direction, assume that \mathcal{L}' is a $(1, 1, \lambda)$ -covering sublattice of A_n . Observe the quotient group $G = A_n / \mathcal{L}'$, and take $D = \{d_0, d_1, \dots, d_n\} \subseteq G$, where $d_i = [\mathbf{f}_{i,0}] \equiv \mathbf{f}_{i,0} + \mathcal{L}'$ are cosets (elements of G). Let us first assure that all the d_i 's are distinct. Suppose that $d_s = d_t$ for some $s \neq t$. This implies that $d_s - d_t = [\mathbf{f}_{s,t}] = [\mathbf{0}]$, which means that $\mathbf{f}_{s,t} \in \mathcal{L}'$. But since $\mathbf{0} \in \mathcal{L}'$, and $\mathbf{0}$ and $\mathbf{f}_{s,t}$ are at distance 1, this would contradict the fact that \mathcal{L}' is independent. Hence, $|D| = n + 1$. Now take any nonzero element of G , say $[\mathbf{y}]$, $\mathbf{y} \notin \mathcal{L}'$. By assumption, \mathbf{y} is covered by exactly λ elements of \mathcal{L}' , i.e., $\mathbf{y} + \mathbf{f}_{s,t} \in \mathcal{L}'$ for exactly λ vectors $\mathbf{f}_{s,t}$. Since $\mathbf{f}_{s,t} = \mathbf{f}_{s,0} - \mathbf{f}_{t,0}$, this means that $d_t - d_s = [\mathbf{f}_{t,0}] - [\mathbf{f}_{s,0}] = [\mathbf{y}]$ for exactly λ pairs (s, t) . D is therefore a $(v, n + 1, \lambda)$ -difference set. ■

Geometrically, the theorem states that balls of radius 1 around the points of the sublattice \mathcal{L} overlap in such a way that every point that does not belong to \mathcal{L} is covered by exactly λ balls. (The points in \mathcal{L} – centers of the balls – are covered by one ball only, and hence this notion is different than that of multitiling [19].)

Example 3. $D = \{0, 1, 2\}$ is a $(4, 3, 2)$ -difference set in the cyclic group \mathbb{Z}_4 . A $(1, 1, 2)$ -covering sublattice $\mathcal{L} \subset A_2$ corresponding to this difference set is illustrated in Fig. 6. Points in \mathcal{L} are depicted as black, and those in $A_2 \setminus \mathcal{L}$ as white dots. For illustration, Fig. 7 shows an example of a $(1, 3, 2)$ -covering sublattice (which does not correspond to any difference set). \triangle

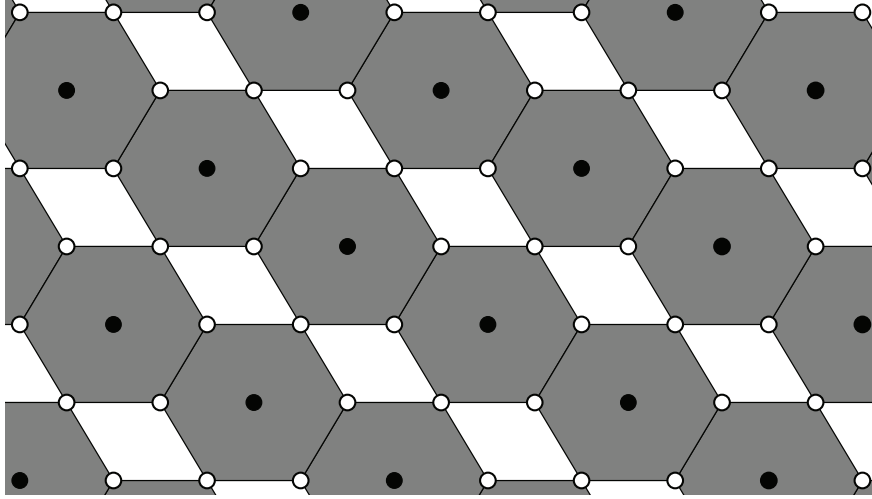


FIGURE 6. A $(1, 1, 2)$ -covering sublattice of A_2 .

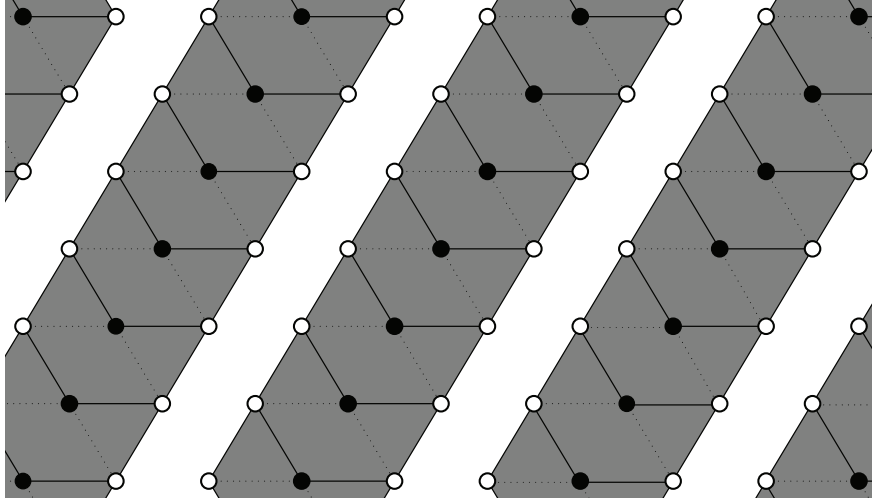


FIGURE 7. A $(1, 3, 2)$ -covering sublattice of A_2 .

Remark 4.2. We can interpret the lattice \mathcal{L} as an error-correcting/detecting code, as before. When $\lambda = 1$, the code can correct a single error because balls of radius one around codewords do not overlap and the minimum distance of the code is three (here by a single error we mean the addition of a vector $\mathbf{f}_{i,j}$ for some i, j , $i \neq j$, to the “transmitted” codeword $\mathbf{x} \in \mathcal{L}$). For $\lambda > 1$, however, it can only *detect* a single error reliably. Note also

that increasing λ increases the density of the code/lattice \mathcal{L} in A_{k-1} , but does not affect its error-detection capability. The densest such lattice is therefore obtained for $\lambda = k$ (that this is the maximum value follows from $\lambda(v-1) = k(k-1)$ and $k \leq v$); it corresponds to the trivial (v, v, v) -difference set $D = G$ in an arbitrary Abelian group G . \triangle

Note that, as in (2.1), we have not specified the order of the elements of D when defining the corresponding lattice \mathcal{L} in (4.1) because it would affect it in an insignificant way only. Note also that if we write $d'_i = zd_i + g$ instead of d_i in (4.1), where z is a fixed integer coprime with v and g is a fixed element of G , identical lattice is obtained because

$$(4.2) \quad \sum_{i=0}^n x_i d_i = 0 \quad \Leftrightarrow \quad \sum_{i=0}^n x_i d'_i = 0$$

which follows from $\sum_{i=0}^n x_i = 0$ and $\gcd(z, v) = 1$.

Let us recall some terminology. Two difference sets D and D' in an Abelian group G are said to be equivalent [5, Rem. 1.11, p. 302] if $D' = \{zd + g : d \in D\}$, for some $z \in \mathbb{Z}$ coprime with v and some $g \in G$. Two codes \mathcal{C} and \mathcal{C}' of length m over an alphabet \mathbb{A} are equivalent [33, p. 40] if there exist m permutations of \mathbb{A} , π_1, \dots, π_m , and a permutation σ over $\{1, \dots, m\}$ such that

$$(4.3) \quad \mathcal{C}' = \{\sigma(\pi_1(x_1), \dots, \pi_m(x_m)) : (x_1, \dots, x_m) \in \mathcal{C}\}.$$

We then have the following:

Proposition 4.3. *If two difference sets D and D' are equivalent, then the corresponding codes (defined as in (4.1)) are equivalent.* \blacksquare

In fact, the π_i 's are necessarily identity maps, only σ is relevant here.

5. CONCLUDING REMARKS

Codes in A_n lattices and, more generally, packings in (\mathbb{Z}^n, d_a) were shown to be well-motivated problems. Certain aspects of the problems, primarily in the linear case, were studied – their connection to B_h sets and difference sets, bounds on the dimension n , packing radius r , and packing density $\mu_n(r)$, as well as the existence of perfect codes.

The results can also be seen as putting B_h sets and difference sets in a more general context. For example, we have seen that B_h sets are, in a certain sense, equivalent to lattice packings of the shapes $S_n(r^+, r^-)$ in \mathbb{Z}^n . From the coding theoretic and geometric point of view, however, there is no reason to restrict oneself to lattice packings. Packings (possibly non-linear) of these shapes represent therefore a generalization of B_h sets. It is an interesting, though apparently very difficult problem to determine the largest possible packing density, and that achievable by lattice packings only, in the asymptotic regimes $r \rightarrow \infty$ and $n \rightarrow \infty$. Of course, it is possible that the two quantities can be compared, perhaps proved equal, without actually determining their values.

ACKNOWLEDGMENT

The author would like to thank Dr Moshe Schwartz, for reading the original manuscript and providing several useful comments, Dr Čedomir Stefanović, the discussions with whom have inspired some of the results on B_h sets, and the anonymous reviewers, whose suggestions have led to a substantial improvement in the content and the presentation of this work.

REFERENCES

1. M. D. Atkinson, N. Santoro, and J. Urrutia, "Integer Sets with Distinct Sums and Differences and Carrier Frequency Assignments for Nonlinear Repeaters," *IEEE Trans. Commun.*, vol. 34, no. 6, pp. 614–617, Jun. 1986.
2. M. A. Axenovich, "On Multiple Coverings of the Infinite Rectangular Grid with Balls of Constant Radius," *Discrete Math.*, vol. 268, no. 1–3, pp. 31–48, Jul. 2003.
3. D. W. Bange, A. E. Barkauskas, and P. J. Slater, "Efficient Dominating Sets in Graphs," in: R. D. Ringeisen and F. S. Roberts (eds.), *Applications of Discrete Mathematics*, SIAM, Philadelphia, 1988, pp. 189–199.
4. A. Barg and A. Mazumdar, "Codes in Permutations and Error Correction for Rank Modulation," *IEEE Trans. Inform. Theory*, vol. 56, no. 7, pp. 3158–3165, Jul. 2010.
5. T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd ed., Cambridge University Press, 1999.
6. R. C. Bose and S. Chowla, "Theorems in the Additive Theory of Numbers," *Comment. Math. Helv.*, vol. 37, no. 1, pp. 141–147, Dec. 1962.
7. S. Buzaglo and T. Etzion, "Tilings with n -Dimensional Chairs and Their Applications to Asymmetric Codes," *IEEE Trans. Inform. Theory*, vol. 59, no. 3, pp. 1573–1582, Mar. 2013.
8. Y. Cassuto, M. Schwartz, V. Bohossian, and J. Bruck, "Codes for Asymmetric Limited-Magnitude Errors with Application to Multilevel Flash Memories," *IEEE Trans. Inform. Theory*, vol. 56, no. 4, pp. 1582–1595, Apr. 2010.
9. S. Chen, "On the Size of Finite Sidon Sequences," *Proc. Amer. Math. Soc.*, vol. 121, no. 2, pp. 353–356, Jun. 1994.
10. J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Springer, 1999.
11. S. I. R. Costa, M. Muniz, E. Agustini, and R. Palazzo, "Graphs, Tessellations, and Perfect Codes on Flat Tori," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2363–2377, Oct. 2004.
12. H. Derksen, "Error-Correcting Codes and B_h -Sequences," *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 476–485, Mar. 2004.
13. C. Ding, *Codes from Difference Sets*, World Scientific, 2015.
14. T. Etzion, "Sequence Folding, Lattice Tiling, and Multidimensional Coding," *IEEE Trans. Inform. Theory*, vol. 57, no. 7, pp. 4383–4400, Jul. 2011.
15. M. Gadouleau and A. Goupil, "A Matroid Framework for Noncoherent Random Network Communications," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1031–1045, Feb. 2011.
16. S. Galovich and S. Stein, "Splittings of Abelian Groups by Integers," *Aequationes Math.*, vol. 22, no. 1, pp. 249–267, 1981.
17. S. W. Golomb and L. R. Welch, "Perfect Codes in the Lee Metric and the Packing of Polyominoes," *SIAM J. Appl. Math.*, vol. 18, no. 2, pp. 302–317, Mar. 1970.
18. R. L. Graham and N. J. A. Sloane, "Lower Bounds for Constant Weight Codes," *IEEE Trans. Inform. Theory*, vol. 26, no. 1, pp. 37–43, Jan. 1980.
19. N. Gravin, S. Robins, and D. Shiryayev, "Translational Tilings by a Polytope, with Multiplicity," *Combinatorica*, vol. 32, no. 6, pp. 629–648, Dec. 2012.
20. W. Hamaker, "Factoring Groups and Tiling Space," *Aequationes Math.*, vol. 9, no. 2-3, pp. 145–149, 1973.
21. D. Hickerson, "Splittings of Finite Groups," *Pacific J. Math.*, vol. 107, no. 1, pp. 141–171, 1983.
22. P. Horak, "Tilings in Lee Metric," *European J. Combin.*, vol. 30, no. 2, pp. 480–489, Feb. 2009.
23. P. Horak, "On Perfect Lee Codes," *Discrete Math.*, vol. 309, no. 18, pp. 5551–5561, Sep. 2009.
24. X.-D. Jia, "On Finite Sidon Sequences," *J. Number Theory*, vol. 44, no. 1, pp. 84–92, May 1993.
25. W. F. Klostermeyer, "A Taxonomy of Perfect Domination," *J. Discrete Math. Sci. Cryptogr.*, vol. 18, no. 1-2, pp. 105–116, 2015.
26. T. Kløve, "Error Correcting Codes for the Asymmetric Channel," Technical Report, Dept. of Informatics, University of Bergen, 1981. (Updated in 1995.)
27. M. Kovačević and P. Popovski, "Zero-Error Capacity of a Class of Timing Channels," *IEEE Trans. Inform. Theory*, vol. 60, no. 11, pp. 6796–6800, Nov. 2014.
28. M. Kovačević and D. Vukobratović, "Perfect Codes in the Discrete Simplex," *Des. Codes Cryptogr.*, vol. 75, no. 1, pp. 81–95, Apr. 2015.
29. M. Kovačević and D. Vukobratović, "Multiset Codes for Permutation Channels," preprint available at arXiv:1301.7564.
30. M. Langberg, M. Schwartz, and E. Yaakobi, "Coding for the ℓ_∞ -Limited Permutation Channel," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Hong Kong, June 2015, pp. 1936–1940.
31. A. W. Lam and D. V. Sarwate, "On Optimum Time-Hopping Patterns," *IEEE Trans. Commun.*, vol. 36, no. 3, pp. 380–382, Mar. 1988.

32. V. I. Levenshtein, "Binary Codes with Correction for Deletions and Insertions of the Symbol 1" (In Russian), *Probl. Peredachi Inf.*, vol. 1, no. 1, pp. 12–25, 1965.
33. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
34. C. Martínez, R. Beivide, and E. Gabidulin, "On the Perfect t -Dominating Set Problem in Circulant Graphs and Codes over Gaussian Integers," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Adelaide, Australia, Sep. 2005, pp. 254–258.
35. P. McMullen, "Convex Bodies Which Tile Space by Translation," *Mathematika*, vol. 27, no. 1, pp. 113–121, Jun. 1980.
36. J. J. Metzner, "Simplification of Packet-Symbol Decoding With Errors, Deletions, Misordering of Packets, and No Sequence Numbers," *IEEE Trans. Inform. Theory*, vol. 55, no. 6, pp. 2626–2639, Jun. 2009.
37. H. Minkowski, "Allgemeine Lehrsätze über Convexen Polyeder" (in German), *Nachr. K. Acad. Wiss. Göttingen, Math.-Phys. Kl. ii*, pp. 198–219, 1897.
38. K. O'Bryant, "A Complete Annotated Bibliography of Work Related to Sidon Sequences," *Electron. J. Combin.*, #DS11, 39 pp. (electronic), 2004.
39. L. J. Schulman and D. Zuckerman, "Asymptotically Good Codes Correcting Insertions, Deletions, and Transpositions," *IEEE Trans. Inform. Theory*, vol. 45, no. 7, pp. 2552–2557, Nov. 1999.
40. M. Schwartz, "Quasi-Cross Lattice Tilings with Applications to Flash Memory," *IEEE Trans. Inform. Theory*, vol. 58, no. 4, pp. 2397–2405, Apr. 2012.
41. S. Sidon, "Ein Satz über Trigonometrische Polynome und Seine Anwendung in der Theorie der Fourier-Reihen" (in German), *Math. Ann.*, vol. 106, no. 1, pp. 536–539, 1932.
42. J. Singer, "A Theorem in Finite Projective Geometry and Some Applications to Number Theory," *Trans. Amer. Math. Soc.*, vol. 43, pp. 377–385, 1938.
43. S. Stein, "Factoring by Subsets," *Pacific J. Math.*, vol. 22, no. 3, pp. 523–541, 1967.
44. S. Stein, "Algebraic Tiling," *Amer. Math. Monthly*, vol. 81, pp. 445–462, May 1974.
45. S. Stein, "Packings of R^n by Certain Error Spheres," *IEEE Trans. Inform. Theory*, vol. 30, no. 2, pp. 356–363, Mar. 1984.
46. S. Stein and S. Szabó, *Algebra and Tiling: Homomorphisms in the Service of Geometry*, The Mathematical Association of America, 1994.
47. J. A. Telle, "Complexity of Domination-Type Problems in Graphs," *Nordic J. Comput.*, vol. 1, pp. 157–171, 1994.
48. R. R. Varshamov, "A Class of Codes for Asymmetric Channels and a Problem from the Additive Theory of Numbers," *IEEE Trans. Inform. Theory*, vol. 19, no. 1, pp. 92–95, Jan. 1973.

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING, NATIONAL UNIVERSITY OF SINGAPORE.
 E-mail address: `mladen.kovacevic@nus.edu.sg`